Concordia Law Review

Volume 3
Number 1 *Concordia Law Review*

Article 5

2018

Bounded by the Constitution: Resolving the Private Search Doctrine Circuit Split

Mark Kifarkis
Chicago-Kent College of Law, mkifarki@kentlaw.iit.edu

BOUNDED BY THE CONSTITUTION: RESOLVING THE PRIVATE SEARCH DOCTRINE CIRCUIT SPLIT

Mark Kifarkis[*]

This Article analyzes the private search doctrine exception to the Fourth Amendment and the exception's application to smart phones and computers. The private search doctrine allows governmental authorities to replicate a private individual's search without obtaining a warrant. This Article proposes a standard for court's to use to resolve the circuit split on how to apply the exception to today's technology. Presently, there are two standards used by courts. The Article names one standard as the "boundless search approach" that is used by the Fifth and Seventh Circuits. The Article names the other standard as "bounded search approach" that is used by Sixth and Eleventh Circuits. The Article proposes courts to use the bounded search approach when reviewing matters regarding the private search doctrine, and an alternative approach that this Article names the "severity of the crime approach."

INTRODUCTION.....144
I. THE FOURTH AMENDMENT AND THE PRIVATE SEARCH DOCTRINE 146
A. Brief Introduction to the Fourth Amendment 146
B. The Private Search Doctrine.....148
1.Governmental Influence Upon the Private Search.....149
2.Scope of the Search.....152
II. THE COURT'S APPLICATION OF THE PRIVATE SEARCH DOCTRINE TO SMARTPHONES AND COMPUTERS 155
A. The Boundless Search Approach 156
1.Fifth Circuit – United States v. Runyan.....157
2.Seventh Circuit – Rann v. Atchison.....159
B. The Bounded Search Approach.....160
1. Sixth Circuit – United States v. Lichtenberger 161
2. Eleventh Circuit – United States v. Sparks.....162
III. COURTS SHOULD ADOPT THE BOUNDED SEARCH APPROACH WHEN REVIEWING MATTERS REGARDING THE PRIVATE SEARCH DOCTRINE 164

[*]J.D., Chicago-Kent College of Law, 2017; B.A., Roosevelt University; Attorney at Beermann Pritikin Mirabelli Swerdlove, LLP. I would like to thank Professor Elizabeth De Armond of Chicago-Kent College of Law for overseeing this Article. I would like to thank the entire staff of Concordia Law Review for their hardwork work in editing this Article. Lastly, I would like to thank Kristyn Rossetti for all of her support.

A. The Bounded Search Approach Better Protects Privacy in Today's Technological Advancements 165
B. Alternatively, a Severity of the Crime Approach Should be Adopted by Courts When Applying the Private Search Doctrine..167
CONCLUSION 168

INTRODUCTION

The amount of private and personal data that can be stored on a smartphone is extraordinary. One of the top-selling smartphones in the world has the capacity to hold 81 films, 229 television shows, 19,125 photos, or 4,080 applications.[1] Technology companies understand the amount of personal data that could be stored on a smartphone and have resisted demands from the government to unlock phones of alleged terrorists, due to the "chilling" effect such a breach of privacy might have.[2] However, a person does not need to be in the technology industry to understand the vast amount of data a smartphone can hold and the number of uses a smartphone can have. In *Riley v. California*, the United States Supreme Court observed that smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and in fact labeled smartphones "minicomputers."[3] Throughout the opinion, Chief Justice Roberts describes smartphones as having immense storage capacity, where a 16-gigabyte smartphone has the ability to hold "millions of pages of text, thousands of pictures, or hundreds of videos."[4] Having smartphones in the palms of people's hands has benefited society in many aspects of daily life, including business, education, health, and social life.[5] Because smartphones are such an integral part of our lives, keeping the information on those devices private is a great concern.[6]

---

[1] David Price, *What's the True Formatted Storage Capacity of an iPhone, iPad or iPod?*, MACWORLD (Feb. 9, 2016), http://www.macworld.co.uk/feature/ipad/whats-iphone-ipod-ipads-true-formatted-storage-capacity-3511773/.
[2] Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.
[3] Riley v. California, 134 S. Ct. 2473, 2489 (2014).
[4] *Id*.
[5] Muhammad Sarwar & Tariq Rahim Soomro, *Impact of Smartphone's on Society*, 98 EUR. J. SCI. RES. 216, 218 (2013).
[6] *Id*. at 224.

Privacy is an issue that many Americans believe is important: they believe that they should be able to maintain privacy and confidentiality in the commonplace activities of their lives.[7] The fear of privacy invasions relating to smartphones is significant, considering that nearly 50% of American adults own a smartphone.[8] Though the Fourth Amendment of the United States Constitution protects against unreasonable search and seizure,[9] the circuits are split on how to apply those protections to computers through a concept known as the private search doctrine.[10] The various court holdings on either side of this split can be similarly applied to smartphones. Smartphone chipmaker ARM believes that, with their newly announced chips, individuals will be able to do all the tasks that currently require a computer.[11] Considering the downward trend of the PC industry and the continued growth of smartphones, it is only a matter of time before smartphones replace computers and tablets.[12]

Furthermore, the Court in *Riley* only briefly discussed the technology that is known as "cloud computing." In dicta, Chief Justice Roberts stated that "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."[13] The Court went on to compare a search of cloud-based storage through a cell phone to "finding a key in a suspect's

---

[7] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. In fact, in a 2015 survey, 95% of adults stated that being in control of who can get information about them is important and 74% felt that it was very important. *Id.* Ninety percent of the adults surveyed that controlling what information is collected about them is important and 65% thought it was very important. *Id.*

[8] The Editorial Board, *Smartphones and the 4th Amendment*, N.Y. TIMES (Apr. 27, 2014), http://www.nytimes.com/2014/04/28/opinion/smartphones-and-the-4th-amendment.html.

[9] U.S. CONST. amend. IV.

[10] Orin Kerr, *11th Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/02/11th-circuit-deepens-the-circuit-split-on-applying-the-private-search-doctrine-to-computers/?utm_term=.882a2009d672.

[11] Christina Bonnington, *In Less Than Two Years, a Smartphone Could Be Your Only Computer*, WIRED (Feb. 10, 2015, 3:42 AM), https://www.wired.com/2015/02/smartphone-only-computer/.

[12] *Id.* Based on the similarities between computers and smartphones, when this Article applies a doctrine to computers it also applies the doctrine to smartphones.

[13] Riley v. California, 134 S. Ct. 2473, 2491 (2014).

pocket and arguing that it allowed law enforcement to unlock and search a house."[14]

Applying the Fourth Amendment to society's advanced technology has challenged the courts.[15] Because computers and smartphones have similar capabilities and storage, the same standard should be applied to both technologies.[16] Part I of this Article provides a brief history of the Fourth Amendment and the warrantless search exception known as the private search doctrine. Part II of this Article discusses the current circuit split between the Fifth and Seventh Circuits on one hand and the Sixth and Eleventh Circuits on the other, concerning what standard to apply to computers and smartphones. Lastly, Part III of this Article offers a resolution to the circuit split that presently exists regarding the applicable standards for smartphones and computers, by adopting what this Article calls the "bounded search approach." If the courts reject this approach, Part III profits an alternative approach to resolving the circuit split that considers the severity of the crime to determine which approach should be applied in a given scenario.

I. THE FOURTH AMENDMENT AND THE PRIVATE SEARCH DOCTRINE

A. *Brief Introduction to the Fourth Amendment*

The Fourth Amendment to the United States Constitution provides for "the right of the people to be secure against unreasonable searches and seizures in their persons, houses, papers, and effects."[17] Furthermore, the Fourth Amendment requires that warrants shall be issued only upon showing probable cause and describing the place to be searched or persons or things to be seized.[18] The Fourth Amendment has an extensive case law history:[19] in the most seminal case, *United States v. Katz*, the Supreme Court held that

---

[14] *Id.*
[15] Kelly A. Borchers, *Mission Impossible: Applying Arcane Fourth Amendment Precedent to Advanced Cellular Phones*, 40 VAL. U. L. REV. 223, 225 (2005).
[16] *Id.* at 257.
[17] U.S. CONST. amend. IV.
[18] *Id.*
[19] *See e.g.*, *A Selection of Supreme Court Cases Involving the Fourth Amendment & the Body*, A.B.A., https://search.americanbar.org/search?q=A+Selection+of+Supreme+Court+Cases+Involving+the+Fourth+Amendment+%26+the+Body&client=default_frontend&proxystylesheet=default_frontend&site=default_collection&output=xml_no_dtd&oe=UTF-8&ie=UTF-8&ud=1&getfields=gsaentity_aba_collection (follow "[MS WORD] A Selection of Supreme Court" hyperlink) (last visited Jan. 20, 2018).

a search occurs when the government violates a subjective expectation of privacy that society considers objectively reasonable.[20] This is otherwise known as the *Katz* reasonable expectation of privacy test.[21] The test to determine whether an individual has a reasonable expectation of privacy has two prongs: one that is subjective and one that is objective.[22] The subjective prong requires a reasonable expectation in the mind of the defendant, while the objective prong requires that society must consider the defendant's subjective expectation of privacy to be reasonable.[23] In *Katz*, the Court rejected the notion that only certain physical areas are constitutionally protected and established the dual prong reasonable expectation of privacy test.[24]

Although a warrant is typically required by authorities to perform a Fourth Amendment search, certain exceptions allow the government to circumvent the warrant requirement.[25] In *Katz*, the Court stated:

> "Over and again this Court has emphasized that the mandate of the (Fourth) Amendment requires adherence to the judicial process" . . . and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment–subject only to a few specifically established and well delineated exceptions.[26]

The Court created an exception to this rule in *Riley*, holding that a warrantless search could be permitted through balancing "on the one hand, the degree to which it intrudes upon an individual's privacy, and on the other hand, the degree to which it is needed for the promotion of legitimate governmental interests."[27] Another exception is the third-party doctrine, which states:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to [g]overnment authorities, even if the information is revealed

[20] Katz v. United States, 389 U.S. 347, 361 (1967).
[21] *Id.*
[22] Borchers, *supra* note 15.
[23] *Katz*, 389 U.S. at 361.
[24] Michael Wukmer, Comment, *The Fourth Amendment Following Private Searches: Is There a Privacy Interest to Protect?*, 52 U. CIN. L. REV. 172, 176–80 (1983).
[25] *Katz*, 389 U.S. at 357.
[26] *Id.* (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)).
[27] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

> on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[28]

Other well-established exceptions, including searches incident to a lawful arrest, searches authorized by consent, hot pursuit, plain view observation, and customs searches, were created by the Court because the Court determined in each case that not all warrantless searches are unreasonable.[29] The private search doctrine should stand amidst these various exceptions.

B. *The Private Search Doctrine*

The protection provided through the Fourth Amendment and the Constitution only insulate the public from government actions.[30] The Fourth Amendment's "origin and history clearly shows that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies."[31] Thus, if a search or seizure was carried out by a private citizen who was not acting as an agent of the government, the Fourth Amendment would not apply, regardless of the unreasonableness of the search.[32]

Under the private search doctrine, governmental authorities may retrace a private individual's search without obtaining a warrant[33] because the owner's reasonable expectation of privacy has already been breached.[34] The private search doctrine finds its roots in *United States v. Jacobsen*.[35] For a search to fall within the private search doctrine the government must establish that: (1) the government did not influence the private citizen to conduct the search, and (2) the subsequent governmental search did not exceed the scope of the private search.[36] The Fourth Amendment limitations will be fulfilled if the government meets these two elements. The following sections analyze each element of the private search doctrine.

---

[28] United States v. Miller, 425 U.S. 435, 443 (1976).
[29] Kim A. Lambert, United States v. Jacobsen: *Expanded Private Search Doctrine Undermining Fourth Amendment Values*, 16 LOY. U. CHI. L.J. 359, 364–65 (1985).
[30] United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[31] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).
[32] *Jacobsen*, 466 U.S. at 113.
[33] United States v. Spicer, 432 F. App'x 522, 523 (6th Cir. 2011).
[34] Andre MacKie-Mason, *The Private Search Doctrine After* Jones, 126 YALE L.J.F. 326 (2017), http://www.yalelawjournal.org/forum/the-private-search-doctrine-after-jones.
[35] *Spicer*, 432 F. App'x at 523.
[36] Wukmer, *supra* note 24, at 176–80.

1. Governmental influence upon the private search. The first prong of the private search doctrine requires a court to determine if the government was involved in or influenced the private search.[37] In order for there to be government influence or involvement, the government authorities need not actually be present at the time and place of the citizen's search.[38] No bright line test reveals when the government involvement goes too far.[39] Rather, the courts adjudicate Fourth Amendment challenges on a case-by-case basis, examining the particular facts of each case to determine whether government influence necessitates application of the Fourth Amendment.[40] For example, searches conducted by a private person who was encouraged or directed by government officials and searches where the private person is actually an informant constitute sufficient government influence to implicate the Fourth Amendment.[41] Two critical factors in assessing whether a private party acts as an agent of the government are: (1) the government's knowledge of and acquiescence to the search, and (2) the intent of the party performing the search.[42]

United States v. Parker provides an example of governmental influence that is insufficient to implicate the Fourth Amendment in a private search. In *Parker*, a UPS employee opened a package that was insured for $4,000, to ensure it conformed to UPS's policy for packages insured for more than $1,000.[43] The UPS employee discovered $4,000 in the case and notified the United States Drug Enforcement Administration (DEA), which then asked UPS to ship the package and notify them of any return package.[44] However, the DEA never inspected the package.[45] UPS then informed the DEA of a return package and delivered it to the DEA's office.[46] There, a drug dog indicated the package contained narcotics.[47] The DEA then obtained a

---

[37] *Jacobsen*, 466 U.S. at 117.
[38] WILLIAM E. RINGEL, SEARCHES AND SEIZURES, ARRESTS AND CONFESSIONS § 2:3 (2d ed. 2017).
[39] United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003).
[40] *Id.*
[41] Ringel, *supra* note 38.
[42] United States v. Malbrough, 922 F.2d 458, 462 (8th Cir. 1990) (quoting United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982)).
[43] United States v. Parker, 32 F.3d 395, 397 (8th Cir. 1994).
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*

warrant to open the package and found over 100 grams of methamphetamine.[48] On appeal, the defendants argued that UPS was operating as an agent of the government when UPS employees cooperated with the DEA, since the employees' actions furthered only the interests of the government.[49] The DEA countered that no government entity directed UPS to open the first package; UPS opened the package pursuant to its own company policy.[50] The Eighth Circuit sided with the DEA, holding that UPS opened the package on their own accord with no influence from the government, and the DEA opened the package only after it had obtained a search warrant.[51] In *Parker*, the DEA did not go beyond the scope of the private search because it did not handle the first package at all, and it did not open the second package until it obtained a search warrant. Had the DEA opened and searched the second package without obtaining a search warrant, it would have expanded the scope of the private search by doing more than the employee did, which would have implicated the Fourth Amendment.

Where the government influences or encourages private parties to conduct searches, the searches may fall outside the private search doctrine and, thus, be subject to Fourth Amendment protection. Governmental influence on a private party defeats the idea that a private search is truly conducted by a private party: rather, it is a private party conducting a search at the behest of the government. This scenario is evident in *Skinner v. Railway Labor Executives' Ass'n*. The Federal Railroad Safety Act of 1970 authorized the Secretary of Transportation to "prescribe, as necessary, appropriate rules, regulations, orders, and standards for all areas of railroad safety," after data revealed that alcohol and drug abuse by railroad employees posed a serious threat to public safety.[52] The Federal Railroad Administration (FRA) subsequently circulated regulations that mandated blood and urine tests of employees who were involved in certain train accidents and that authorized, but did not require, railroads to administer breath and urine tests to employees who violated certain rules.[53]

---

[48] *Id.*
[49] *Id.* at 398.
[50] *Id.* at 399.
[51] *Id.*
[52] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 606 (1989).
[53] *Id.*

Skinner required the Supreme Court to determine whether these blood and urine test regulations violated the Fourth Amendment.[54] The Court held that a search is not automatically private if the government has not compelled a private party to perform the search.[55] In *Skinner*, the specific features of the regulations convinced the Court that the government did more than adopt a passive position toward the underlying private conduct by the railroad companies.[56] The Court recognized government influence because the regulations set forth in Subpart D by the FRA pre-empted state laws, rules, or regulations covering the same subject matter and were intended to supersede any provision of a collective bargaining agreement or arbitration award construing such an agreement.[57] Furthermore, the Court found that the regulations also conferred upon the FRA the right to receive certain biological samples and test results procured by railroads pursuant to Subpart D.[58] Finally, a railroad could not divest itself of, or otherwise compromise by contract, the authority conferred by Subpart D.[59] In light of all these provisions, the Court was unwilling to accept the government's argument that the tests conducted by private railroads in reliance on Subpart D were primarily the result of private initiative, because the government removed all legal barriers to the testing and had made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions.[60]

Based upon these two cases, it is clear that the private search doctrine applies only when governmental authorities do not influence or compel a private citizen to conduct the search on behalf of the government. Essentially, if the government has encouraged, endorsed, or participated in any way in a search conducted by a private citizen, a court will find that there is enough governmental influence to implicate the Fourth Amendment.

---

[54] *Id.* at 614.
[55] *Id.* at 615.
[56] *Id.*
[57] *Id.* Subpart D authorizes but does not require railroads to administer breath or urine tests or both to covered employees who violate certain safety rules. *Id.* Furthermore, Subpart D makes plain a strong preference for testing and a governmental desire to share the fruits of such intrusions and the regulation mandates that railroads not bargain away their Subpart D testing authority. *Id.*
[58] *Id*.
[59] *Id.*
[60] *Id.*

2. Scope of the search. The second prong of the private search doctrine requires that the scope of the governmental authority's search must not exceed the scope of the private party's search. Three cases clearly illustrate the contours of this prong. In United States v. Jacobsen, the employees of a private freight carrier noticed a white powdery substance that was originally concealed within eight layers of wrappings.[61] The employees called a federal agent, who tested the powder using a chemical test that revealed the powder was cocaine.[62] The Supreme Court was tasked with determining if, pursuant to the Fourth Amendment, the agent was required to obtain a warrant before he tested the substance.[63] The Court held that once a private search has been performed, it eradicates the individual's reasonable expectation of privacy.[64] Once this happens, "the Fourth Amendment does not prohibit governmental use of the now non-private information."[65] However, once the governmental authorities conduct their own search, they must not exceed the scope of the private search without obtaining a warrant.[66]

The second case, *Walter v. United States*, best illustrates the issue of police exceeding the scope of the private search.[67] In *Walter*, employees of L'Eggs Products, Inc. opened a dozen cartons of homosexual motion pictures that were accidentally shipped to them and found that the individual boxes depicted suggestive drawings and explicit descriptions of the contents.[68] After an employee opened one or two of the boxes and attempted to view the film, the employees called the FBI.[69] Upon retrieving the packages, the agents viewed the films without obtaining a warrant, and the petitioners were indicted with obscenity charges.[70]

The Court explained that, if the results of the private search are in plain view when the materials are turned over to the government, the government may justify their re-examination of the materials; however, the

---

[61] United States v. Jacobsen, 466 U.S. 109, 111 (1984).
[62] *Id.*
[63] *Id.*
[64] *Id.* at 117.
[65] *Id.*
[66] *Id.* at 116.
[67] 32 LEONARD N. ARNOLD, N.J. PRACTICE SERIES, CRIMINAL PRACTICE AND PROCEDURE § 16:29 (2016–2017 ed.).
[68] Walter v. United States, 447 U.S. 649, 651–52 (1980).
[69] *Id.* at 652.
[70] *Id.*

government may not exceed the scope of the private search unless it has the right to make an independent search.[71]

> In determining whether police officers have exceeded the scope of a private search a court should inquire whether the government learned something from the police search that it could not have learned from the private searcher's testimony and, if so, whether the defendant had a legitimate expectation of privacy in that information.[72]

The Court found that the government action, viewing the films, was a significant expansion of the private party's initial search because the private party had not actually watched the films.[73] The Court therefore characterized the government viewing the films as a separate search.[74]

United States v. Miller further illustrates the private search doctrine's scope requirement. In *Miller*, an employee at a mental illness treatment facility went to the apartment of a patient to give the patient medication, but the employee forgot that the patient was out of town.[75] Upon entering the patient's room using the master key, the employee smelled cigarette smoke, which caused concern because of the facility's strict no smoking rule.[76] The employee saw evidence of both cigarette usage and drug activity all lying out in plain view, and reported what she saw to the director who then called the police.[77] Upon responding to the director's call, police officers observed only the evidence that the employee saw.[78] Based on the officers' observations, the police obtained a search warrant.[79] The defendant appealed, arguing that his Fourth Amendment rights were violated; the government countered arguing third-party consent overcame the Fourth Amendment issue.[80] The Eighth Circuit, *sua sponte*, held that the facility employees' search unquestionably constituted a valid private search.[81] Also, the circuit court

---

[71] *Id.* at 657.
[72] Ringel, *supra* note 38.
[73] *Walter*, 447 U.S. at 657.
[74] *Id.*
[75] United States v. Miller, 152 F.3d 813, 814–15 (8th Cir. 1998).
[76] *Id.* at 815.
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.* at 816.

held that the police did not participate in or influence the employees' entry, and once the police became involved, their intrusion went no further than the private search.[82] The fact that the police became involved did not implicate the Fourth Amendment in *Miller* because the police's intrusion did not exceed the scope of the private search conducted by the facility employees.

It is important to note that there are circumstances where a court is unable to determine whether the government agent exceeded the scope of the private search.[83] In *United States v. D'Andrea*, a tipster called a child abuse hotline and informed the Massachusetts Department of Social Services (DSS) that she had received a message on her mobile phone that contained photographs of the defendants performing sexual acts on D'Andrea's eight-year-old daughter and photos of the daughter's exposed genitalia.[84] The tipster advised DSS how to access the pictures through the mobile phone provider's website.[85] DSS agents reported it to the local police department.[86] Upon accessing the website, DSS agents found numerous pornographic pictures of D'Andrea's daughter.[87] However, due to the record's miniscule detail surrounding the scope of the private search, the Court lacked sufficient evidence to determine whether DSS expanded the scope of the private search.[88]

These cases show how both prongs of the private search doctrine operate. The requirements of no government influence on the private search and no government search beyond the scope of the private search provide an adequate framework even in our rapidly evolving technological era. The next section analyzes the problems of applying the doctrine to smartphones and computers.

---

[82] *Id.*
[83] *See* United States v. D'Andrea, 648 F.3d 1, 9 (1st Cir. 2011) (holding that "the record [did] not provide enough meaningful details on the searches of the websites by the Tipster and the DSS, . . .[the court did] not have enough evidence to determine whether the DSS search of the website exceeded the scope of the tipster's search").
[84] *Id.* at 3–4.
[85] *Id.* at 4.
[86] *Id.*
[87] *Id.*
[88] *Id.* at 9.

II. THE COURT'S APPLICATION OF THE PRIVATE SEARCH DOCTRINE TO SMARTPHONES AND COMPUTERS

The private search doctrine presents a whole new set of problems when it is applied to technology. The primary question that arises is, "when a private party searches a computer, sees a suspicious file and reports the finding to the police, what kind of government search of the computer counts as merely reconstructing the private search and what kind of search counts as exceeding the private search?"[89] This is a difficult issue to answer because the courts face a number of alternatives: "what's the right measuring unit to use – the data, the file, the folder, the physical device, or something else?"[90] An analogous situation exists when the police enter a house: can they search everything inside the house or only what is visible? "The opening of any closed containers inside the house constitutes a separate search."[91] A "closed container" is analogous to a smartphone with multiple photo albums on its camera. Each album is a "closed container" and opening the album would constitute a new search. Courts battling this issue have developed different methods of resolving exactly how much can be searched. Particularly, courts have established two types of standards: the single unit approach (hereinafter called the "boundless" search approach), and the folder approach (hereinafter called the "bounded" search approach).[92]

The Fifth and Seventh Circuits apply the boundless search approach when governmental authorities search a technological device based on the private search doctrine.[93] Thus, both circuits reject the idea that each album, or folder on a computer, is a closed container that constitutes a new search. Instead, these circuits see the device as one container, meaning that one search is all that is needed. On the other hand, the Sixth and Eleventh Circuits apply the bounded search approach when governmental authorities search a

---

[89] Kerr, *supra* note 10.
[90] Orin Kerr, *Sixth Circuit Creates Circuit Split on Private Search Doctrine for Computers*, WASH. POST (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/?utm_term=.60befdca9a6f.
[91] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554 (2005).
[92] Joel Varner, *Computers, the Private Search Doctrine, and the Fourth Amendment*, MICH. TELECOMM. & TECH. L. REV., http://mttlr.org/2015/11/05/computers-the-private-search-doctrine-and-the-fourth-amendment/ (last visited Jan. 20, 2018).
[93] Kerr, *supra* note 10.

device using the private search doctrine.[94] The Sixth and Eleventh Circuits believe that if authorities want to view a new album on a smartphone, or a separate folder on the computer that was not searched by the private search, then a warrant is required because the governmental authorities are bounded to the scope of the private search.

A. *The Boundless Search Approach*

The boundless search approach, or single unit approach, adopted by the Fifth and Seventh Circuits allows governmental authorities to search the entire device or computer.[95] Hence, the authorities are boundless in their search. For example, if a citizen conducts a private search on a smartphone and views only one album of photos out of dozens of albums, the boundless search approach allows governmental authorities to view the contents of the entire smartphone, including all the photos stored in it, not just the one specific album the private citizen viewed. Even though the private citizen may not have viewed each image that was on the smartphone, the Fifth and Seventh Circuits agree that this approach properly balances the governmental interest in potential information to be gained from the search with the smartphone owner's reasonable expectation of privacy in the device.[96] Following this reasoning, these circuits feel that the government's potential ability to gather information outweighs a citizen's reasonable expectation of privacy in their personal electronics.

Questions regarding the scope of the government search arise when the boundless search approach is adopted. However, even though the governmental authorities' search is more thorough than the private search and covers areas that were not viewed by the citizen, the Fifth and Seventh Circuits agree that the governmental search does not exceed the scope of the private search.[97] Accordingly, the search of the entire device complies with the Fourth Amendment, under the Fifth and Seventh Circuits' interpretation of the private search doctrine.

---

[94] *Id.*
[95] Varner, *supra* note 92.
[96] Katie Matejka, United States v. Lichtenberger*: The Sixth Circuit Improperly Narrowed the Private Search Doctrine of the Fourth Amendment in a Case of Child Pornography on a Digital Device*, 49 CREIGHTON L. REV. 177, 192 (2015).
[97] Varner, *supra* note 92.

1. Fifth Circuit – United States v. Runyan. Generally, courts have agreed that governmental searches, initiated by a private search, of computers, smartphones, or other electronic devices must conform to the bounded search approach.[98] However, the Fifth Circuit adopted the boundless search approach for Fourth Amendment purposes to a computer disk containing multiple files.[99] The seminal case for the Fifth Circuit that established its adoption of the boundless search approach arises from United States v. Runyan.[100]

In *Runyan*, the defendant's ex-wife was retrieving her personal property from the defendant's ranch when she and a companion found pornographic photographs they believed to be of a teenager.[101] The two also removed a computer and various electronic storage devices.[102] Her companion then examined several of the storage devices and discovered that some contained images of child pornography, leading the companion to contact the sheriff's department.[103] Through the course of several weeks, the authorities searched additional material from the sources that were turned over by the defendant's ex-wife and her companion—material that was not searched in the private searches.[104]

On its face, the search that the authorities conducted exceeded the scope of the private search that the ex-wife and her companion had originally conducted, and thus would violate the Fourth Amendment. But the Fifth Circuit took the position that "police do not exceed the private search when they examine more items within a closed container than did the private searchers."[105] The closed container was the computer's hard drive, and because the private search exposed some of the files from the container, it left the remaining files, which were not viewed during the private search, open to further inspection.[106] The court reasoned that the authorities were only expanding the prior private search when they opened different files and thus

---

[98] 4 CRIM. PRAC. GUIDE: SEARCHING AND SEIZING COMPUTERS WITHOUT A WARRANT 2 (Mar./Apr. 2003 ed.).
[99] *Id.*
[100] Kerr, *supra* note 10.
[101] United States v. Runyan, 290 F.3d 223, 232 (5th Cir. 2002).
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001).
[106] Kerr, *supra* note 91, at 555.

did not exceed the scope of the private search because the search was still defined by the physical storage devices.[107] The court ruled:

> [P]olice exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise.[108]

Based on the authorities' conversations with the defendant's ex-wife regarding the disks she searched and their contents, the police did not exceed the scope of the private search because they were substantially certain what the disks contained.[109]

However, the court did say the police exceeded the scope of the search when they examined disks that the ex-wife and her companion had never examined at all. The court stated:

> Any evidence that police obtained from a closed container that was unopened by prior private searchers will be suppressed unless they can demonstrate to a reviewing court that an exception to the exclusionary rule is warranted because they were substantially certain of the contents of the container before they opened it.[110]

Therefore, the court found that "[t]he police could not have concluded with substantial certainty that all of the disks contained child pornography based on knowledge obtained from the private searchers, information in plain view, or their own expertise."[111] Apart from the disks the ex-wife examined, there was no evidence as to what the other disks contained (e.g., there were no labels or markings on the disks): thus, the police exceeded the scope of the private search.[112]

---

[107] *Id.*
[108] *Runyan*, 275 F.3d at 463.
[109] *Id.* at 465.
[110] *Id.* at 464.
[111] *Id.*
[112] *Id.*

2. Seventh Circuit – Rann v. Atchison. The Seventh Circuit agrees with the Fifth Circuit's position that the boundless search approach should apply when authorities search a computer or smartphone.[113] The court in Rann v. Atchison adopted the Fifth Circuit's view in Runyan and broadly construed the scope of the private search doctrine.[114] In Atchison, the defendant's 15-year-old daughter reported to police that her father, the defendant, had both sexually assaulted and taken pornographic pictures of her.[115] After being interviewed by the police, she went back home and procured a digital camera memory card from her parents' bedroom and provided it to the police, who subsequently downloaded images depicting the alleged sexual assault.[116] Additionally, the victim's mother brought the police a computer ZIP drive that contained additional pornographic images of the defendant's daughter and stepdaughter.[117] The defendant was convicted on two counts of sexual assault and one count of possession of child pornography.[118] On appeal, the court was tasked with resolving whether the police went beyond the scope of the private search.[119]

The Seventh Circuit took the same view as the Fifth Circuit in *Runyan* and held that, when the private party has searched a single file, the entire physical device is subject to being searched by the government without a warrant.[120] The Fifth Circuit's reasoning in *Runyan* was persuasive to the Seventh Circuit, which adopted it because "[a] defendant's expectation of privacy with respect to a container unopened by the private searchers is preserved unless the defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search."[121]

Essentially, the test goes back to *Katz* to determine if the defendant had a reasonable expectation of privacy in the device. In the eyes of the Fifth and Seventh Circuits, the defendant fails the objective prong of *Katz* because

---

[113] Pierre Grosdidier, *After Riley, Circuits Narrow Private Search Doctrine*, LAW360 (Jan. 11, 2016, 11:15 AM), http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine (on file with *Concordia Law Review*).
[114] *Id.*
[115] Rann v. Atchison, 689 F.3d 832, 834 (7th Cir. 2012).
[116] *Id.*
[117] *Id.*
[118] *Id.* at 833.
[119] *Id.* at 835.
[120] Kerr, *supra* note 91.
[121] *Rann*, 689 F.3d at 837.

the court says there is no reasonable expectation of privacy once a private party has searched a file on the device. Thus, even if the party has not searched any other files on the device, the search of a single file renders the owner's expectation of privacy in any material on the device unreasonable. It is not the subjective prong of *Katz* that fails, because it is reasonable to argue that the defendant would still have a subjective reasonable expectation of privacy in the remaining disks or files after one of them has been open.

In *Atchinson*, the court held that it was reasonable that the police knew the digital media devices contained evidence because both the daughter and the mother brought devices to support the sexual assault allegations.[122] The daughter knew that the defendant has taken pornographic pictures of her and brought the police a memory card that contained those pictures, and the mother brought a ZIP drive containing pornographic pictures of her daughter to support the daughter's allegations.[123] The defendant had no reasonable expectation of privacy in the devices, and therefore, the Fourth Amendment does not apply.[124]

Thus, the Fifth and Seventh Circuits' objective in allowing the boundless search approach is to support the governmental authorities in obtaining evidence against the defendant by allowing the authorities to search the entire device. The Fifth and Seventh Circuits' view is that once a private search has been conducted on a device, there is no reasonable expectation of privacy in that device any longer, thereby allowing authorities to search the entire device. The boundless search approach adopted by the Fifth and Seventh Circuits is beneficial to governmental-authority: the gathering of potential evidence outweighs any expectation of privacy the owner may have.

B. *The Bounded Search Approach*

The private search doctrine, after *Runyan* and *Atchison,* appeared to clearly encompass the boundless search approach.[125] However, the Sixth and Eleventh Circuits did not adopt the boundless search approach; rather, they adopted the approach dubbed the bounded search approach. In 2012, the Sixth Circuit held that the proper approach was to view the data on the

---

[122] *Id.* at 838.
[123] *Id.*
[124] *Id.*
[125] Varner, *supra* note 92.

device as separate files rather than a single data unit.[126] This approach was subsequently adopted by the Eleventh Circuit as well.[127] Under the bounded search approach, if the private search is performed on a smartphone or computer and the private party only opens one specific image or file on the device, then the authorities are bound by the private search and can only open that one image or file. This is in contrast to the boundless search approach, in which there is no question that the authorities would have the ability to search the entire smartphone or computer, regardless of which files were opened by the private party.

1. Sixth Circuit – United States v. Lichtenberger. The Sixth Circuit case that adopts the bounded search approach is United States v. Lichtenberger. In Lichtenberger, the defendant's girlfriend accessed his laptop and began to open different folders, eventually finding child pornography.[128] She then proceeded to show her mother, and the two viewed several more sexually explicit images involving minors before contacting the police.[129] Upon arriving at the residence, the police officer asked the defendant's girlfriend to show him the pictures on the laptop.[130] She showed the officer random photos from several folders.[131] The defendant's girlfriend later testified that she was not sure if the pictures she showed to the officer were among the same pictures she had seen in her original search.[132] The court held that the search by the officer, in which he instructed the defendant's girlfriend to go through the computer again, exceeded the scope of the initial private search.[133] The court held that the officer "must have virtual certainty that reproducing the search will not reveal anything the [officer] did not already know."[134] Because the defendant's girlfriend did not show the officer the exact same images she already viewed, the court reasoned that the officer did not have virtual certainty that he would not have seen something unrelated to the child pornography.[135]

The defendant argued that the private search was unconstitutional because the girlfriend was acting as an agent of the state, and not because the

---

[126] United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015).
[127] United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015).
[128] *Lichtenberger*, 786 F.3d at 480.
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.* at 481.
[133] *Id.* at 485.
[134] Matejka, *supra* note 96, at 180.
[135] *Id.*

scope of the second search exceeded the original search.[136] The Sixth Circuit, although agreeing with the district court's conclusion of suppressing the evidence, disagreed with this agency approach.[137] There was no question that the initial search was private, but the district court erred by determining whether the defendant's girlfriend acted as an agent of the state instead of analyzing the scope of the search itself.[138] The Sixth Circuit found this to be an error, yet still suppressed the evidence because the search exceeded the scope of the initial private search.[139]

Under the Fifth and Seventh Circuits' approach, the officer's search would have been within the scope of the private search, because the search was conducted on the same device as the private search. Thus, even though the officer viewed images that the private searcher did not, it would still be within the scope of the private search under the Fifth and Seventh Circuits' holdings. However, the Sixth Circuit adopted the bounded search approach because of the sensitive nature of the computer, in order to protect private information by limiting governmental authorities' ability to perform such searches without a warrant.

2. Eleventh Circuit – United States v. Sparks. In the most recent decision on these doctrines, the Eleventh Circuit adopted the bounded search approach in United States v. Sparks, bolstering the circuit split by holding that law enforcement is limited to viewing files that a private search has already viewed.[140] Defendants Johnson and Sparks left their cell phone at a Wal-Mart store where an employee searched the contents of the password-less phone and discovered child pornography.[141] The employee showed her fiancé the images, and he scrolled through the thumbnails and viewed a few full size images and a video.[142] After their private search, the couple gave the phone to police officers, whereupon a Sergeant O'Reilly then viewed the thumbnails that the fiancé had viewed, the video that the fiancé viewed, and

---

[136] *Lichtenberger*, 786 F.3d at 481.
[137] *Id.* at 484.
[138] *Id.*
[139] *Id.*
[140] Robert T. Denny, *Warrantless Search of Cell Phones Violates Fourth Amendment*, LITIG. NEWS (May 5, 2016), http://apps.americanbar.org/litigation/litigationnews/mobile/article-search-without-warrant.html.
[141] United States v. Sparks, 806 F.3d 1323, 1329 (11th Cir. 2015).
[142] *Id.* at 1331.

one additional video that was not viewed in the private search.[143] The defendants contended that Sergeant O'Reilly's warrantless search of the cell phone violated their Fourth Amendment rights because he was not within the scope of the search that the private citizens conducted.[144]

The Eleventh Circuit agreed with the defendants and held that the search by law enforcement was an illegal search because the officer viewed more files than the private search.[145] In deciding to adopt the bounded search approach, the Eleventh Circuit found that Sergeant O'Reilly's search was within the scope of the private search when O'Reilly viewed the photos and video that the couple previously viewed.[146] Thus, the Fourth Amendment was not violated.[147] However, when O'Reilly viewed the second video, which the couple never viewed, he exceeded the scope of the private search and violated the Fourth Amendment.[148] The Eleventh Circuit appeared to be influenced by how much information can be stored on the cell phone and the private nature of a cell phone.[149] The court even relied on *Riley*, a non-private search doctrine case.[150] The Eleventh Circuit "stressed the intrusiveness of searching the personal electronic devices, as does Riley, and [held] that a warrantless government search cannot exceed the specified files viewed in a prior private search."[151]

In summary, the Eleventh and Sixth Circuits err on the side of privacy when it comes to the private search doctrine. On the other hand, the Fifth and Seventh Circuits err on the side of law enforcement efficiency when it comes to the private search doctrine. Until the United States Supreme Court decides to hear a case on the private search doctrine, the circuit split will remain and uncertainty will continue as to which method will be adopted by the other circuits—the bounded approach or the boundless approach.

---

[143] *Id.* at 1332.
[144] *Id.* at 1334.
[145] Denny, *supra* note 140.
[146] *Sparks,* 806 F.3d at 1336.
[147] *Id.*
[148] *Id; see also* Kerr, *supra* note 10.
[149] *Sparks,* 806 F.3d at 1336.
[150] *Id.*
[151] Grosdidier, *supra* note 113.

III. COURTS SHOULD ADOPT THE BOUNDED SEARCH APPROACH WHEN REVIEWING MATTERS REGARDING THE PRIVATE SEARCH DOCTRINE

To resolve the circuit split regarding which approach a court should use when applying the private search doctrine, the Supreme Court should adopt the bounded approach in order to protect the individual's privacy. Both approaches have their positives and negatives. The boundless approach allows authorities to inspect the entire cell phone. The primary positive for this approach is that it allows law enforcement to gather additional information beyond what is revealed in the private search, thus potentially preventing further crimes including, in the extreme case, potential terrorist attacks. However, law enforcement is able to gather additional information from the entire device at the expense of the owner's privacy. For example, if law enforcement conducts a search based upon the private search doctrine, but exceeds the scope of the private search only to find photos of the owner's family, the owner's privacy has been completely breached with no benefit realized by law enforcement. The boundless approach allows law enforcement to view all of "the privacies of life" that people store on their smartphones.[152] Furthermore, exceeding the scope of the private search could potentially reveal evidence of an additional crime that is unrelated to the search. Typically, a warrant would be required to find such information, but the boundless search approach allows law enforcement to search without violating the Fourth Amendment. The possibilities of abuse and opportunities for law enforcement to entertain a fishing expedition for whatever they can find are limitless.

On the other hand, the bounded approach protects the privacy of the individual, particularly in cases where the smartphone does not have any additional information related to the crime. Taking the same example that is stated above, but using the bounded search approach, law enforcement would not be able to access "the privacies of life" that could be contained on a smartphone. If law enforcement exceeds the scope of the private search, they violate the Fourth Amendment. The bounded approach protects the individual's privacy and, perhaps more importantly, it prevents officers from abusing their power and going on a fishing expedition to gather additional evidence of new crimes that are unrelated to the private search. As technology continues to improve exponentially, there must be a balance between

[152] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

government overreach and privacy rights. One way to prevent government overreach is by having the courts uniformly adopt the bounded approach. This will protect the individual's privacy rights when all "the privacies of life" are stored on one device.

A. *The Bounded Search Approach Better Protects Privacy in Today's Technological Advancements*

With the advent of cloud-based storage, it has become critical to protect information in the cloud from improper law enforcement search: the bounded search approach is the only doctrine that does so. Instead of accessing information stored on your smartphone or computer's hard drive, cloud computing allows the user to store and access data and programs over the Internet.[153] In addition, cloud computing allows data from numerous devices to be stored in one cloud. Thus, if an individual accesses the cloud through the Internet from a smartphone, data that the user stored on the cloud from other devices will appear.[154] To be clear, this Article does not address the third-party doctrine's application of the Fourth Amendment to cloud storage.[155]

A typical example of a cloud-based storage system is Google Drive. Google Drive gives the user 15 gigabytes of free storage to upload photos, drawings, videos, recordings, and essentially any type of data.[156] Google Drive can be accessed from any smartphone, tablet, or computer.[157] Therefore, wherever users have access to the Internet, they can access the files from their Google Drives. This means that photos uploaded from a computer to Google Drive are accessible from a smartphone as long as the Google Drive app is downloaded.[158] Therein lies the monumental clash between cloud-based storage and the boundless search approach—applying

---

[153] Eric Griffith, *What is Cloud Computing?*, PC (May 3, 2016, 12:01 AM), http://www.pcmag.com/article2/0, 2817,2372163,00.asp. The difference between cloud computing and using your hard drive is that when you store data on the hard drive, everything is physically on the hard drive, and only on that specific device's hard drive.

[154] *Id.*

[155] David A. Couillard, *The Cloud and the Future of the Fourth Amendment*, ARS TECHNICA (Apr. 27, 2010, 12:30 AM), https://arstechnica.com/tech-policy/2010/04/the-cloud-and-the-future-of-the-fourth-amendment/ (discussing that the police do not need a warrant to obtain a list of the phone numbers you have dialed because transactional data is part of the business records of a third party).

[156] GOOGLE, https://www.google.com/drive/ (last visited Jan. 20, 2018).

[157] *Id.*

[158] Griffith, *supra* note 153.

the boundless search approach to devices using cloud-based storage can cause disastrous privacy concerns. If a court adopts the boundless search approach, law enforcement will be able to search everything on the phone instead of merely replicating the private search. If law enforcement accesses the cloud on a smartphone, they will have access, not only to what is on the smartphone's hard drive, but to everything that is uploaded to that individual's cloud. This means that law enforcement has within its reach data that has been uploaded from a computer at home, a computer at work, or a tablet, in addition to the smartphone held by law enforcement. In other words, law enforcement would have access to devices that are completely separate from the device that was searched by the private search via the cloud application that is on that device.

However, if a court were to adopt the bounded search approach, law enforcement would be limited to the scope of the private search. Therefore, if the private search only covered the "Photos" album on the owner's smartphone, law enforcement would be strictly bounded to search only that "Photos" album. The cloud would be off limits because it would be beyond the scope of the private search. Even if the private searcher saw criminal activity within the cloud, law enforcement would still be limited to searching only the folder that the private searcher viewed. This protects the privacy of the smartphone owner because the remainder of his cloud storage is off limits to law enforcement. Essentially, the private searcher would need to view all the files on that individual's cloud for law enforcement to be legally allowed to search the entire cloud as well.

The amount of data that can be stored within the cloud is immense. Google Drive has 15 gigabytes of free storage, Dropbox has 2 gigabytes of free storage, Box has 10 gigabytes of free storage, and OneDrive has 5 gigabytes of free storage.[159] These are only four of the numerous cloud storage providers.[160] In addition, all four of these providers also offer paid cloud services. Google Drive offers 100 gigabytes for $2 per month or 1 terabyte for $10 per month and Dropbox offers 1 terabyte for $10 per

[159] Sarah Mitroff, *OneDrive, Dropbox, Google Drive and Box: Which Cloud Storage Service is Right for You?*, CNET (Feb. 1, 2016, 12:00 PM), https://www.cnet.com/how-to/onedrive-dropbox-google-drive-and-box-which-cloud-storage-service-is-right-for-you/.
[160] *Id.*

month.[161] Box offers 100 gigabytes for $10 per month and OneDrive offers 50 gigabytes for $2 per month.[162] The amount of data that can be stored with these cloud services is practically limitless, particularly with the fee-based plans. With as many as 300 million users on Dropbox, 240 million users on Google Drive, and 250 million users on OneDrive, it is vital that the privacy of these users is protected from the overreach of law enforcement viewing data that is unrelated to a private search.[163]

B. *Alternatively, a Severity of the Crime Approach Should be Adopted by Courts When Applying the Private Search Doctrine*

In the event that courts decline to adopt the bounded search approach, this Article proposes an alternative test: courts should consider the severity of the crime to determine when law enforcement may use the boundless search approach. This new test is a good alternative to the bounded search approach when it comes to protecting the individual's privacy.

For example, if a private searcher goes through another's smartphone and finds a text message and photos of a small amount of marijuana (indicating marijuana use or small-scale distribution) the crime is not severe enough for law enforcement to use the boundless search approach. On the other hand, if a private search of a smartphone reveals legitimate blueprints of a terrorist attack, the crime is clearly severe enough to warrant the boundless search approach and allow law enforcement to sift through the entire smartphone's contents.

Admittedly, this test is not without flaws. There is clearly a gray area as to what crimes would be severe enough to merit the boundless approach. The test is also heavily based on law enforcement's judgment in deciding if the crime meets the requisite severity level. However, this test still protects individuals more than completely adopting the boundless search approach. The test also balances the government's interest in protecting society at large against government overreach into one's privacy. The governmental interest of protecting society does not justify exceeding the scope of a private search of a low-level marijuana dealer's smartphone. The privacy right protected outweighs the harm that is being prevented by exceeding the scope of the

---

[161] *Id.*
[162] *Id.*
[163] Erin Griffith, *Who's Winning the Consumer Cloud Storage Wars?*, FORTUNE (Nov. 6, 2014), http://fortune.com/2014/11/06/dropbox-google-drive-microsoft-onedrive/.

search. Furthermore, there are some guidelines that can help determine whether crimes meet the severity level to validate a boundless search. For example, the Omnibus Crime Control and Safe Streets Act of 1968, otherwise known as the Wiretap Act, prohibits unauthorized interception of wire, oral, or electronic communications by government agencies and establishes procedures for obtaining warrants to authorize wiretapping by the government.[164] However, the Wiretap Act provides an exception to the warrant requirement by allowing law enforcement to intercept communications if it reasonably determines that an emergency situation exists involving activities threatening national security.[165] Similarly, in matters as severe as national security, law enforcement should apply the boundless search approach to private searches. This provides extensive protection of privacy for individuals, because most crimes do not rise to such a level.

Ultimately, however, courts should adopt the bounded search approach because it provides the highest protection to the data that is on the owner's device. Specifically, the bounded search approach is best suited for technology that includes cloud-based storage. Adopting a pure boundless search approach should be avoided at all costs due to the potential abuse by law enforcement. Alternatively, if courts do not adopt the bounded search approach, they should use the severity of the crime test proposed here to help law enforcement determine when it would be reasonable to use the boundless search approach. The severity of the crime test may create situations in which the boundless search approach is still used, but it protects the owner's privacy in cases where the crime is not sufficiently severe.

CONCLUSION

Today's society is heavily dependent on technology. The rise of technology has presented serious problems regarding protection of privacy. Currently, law enforcement can circumvent the Fourth Amendment in cases where the private search doctrine applies, subject to one of the two approaches represented in the current circuit split—the boundless search approach and the bounded search approach. Under the boundless search approach, the authorities can search the entire smartphone or computer,

---

[164] *Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, JUST. INFO. SHARING (Sept. 19, 2013), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.
[165] *Id.*

including cloud storage, once the device is searched privately in any way. On the other hand, under the bounded search approach, the authorities can only open the specific images or files that the private parties opened during their search. In order to protect the "privacies of life" that smartphones hold, the bounded approach should be adopted by all remaining circuits or by the Supreme Court. Without the bounded search, law enforcement would have unlimited access to the individual's data that may be completely unrelated to the private search, whether that data is stored on the smartphone, computer, or in the cloud. As an alternative to the bounded search approach, courts could use a severity of the crime test to determine when the boundless search approach is reasonable, such as for matters of national security. The "privacies of life" deserve the highest possible protection and that protection can only be provided by the bounded search approach when law enforcement circumvents the Fourth Amendment warrant requirement through the private search doctrine.